Privacy-Preserving Surveillance System

Submitted in the partial fulfillment for the award of

the degree of

BACHELOR OF ENGINEERING

IN

CSE(Hons.)- INFORMATION SECURITY

Submitted by:
KARTIK KUMAR- 21BCS8403
PRATEEK MUKHERJEE- 21BCS8404

Under the Supervision of:
Ms. SHEETAL LAROIYA
E-15433

Outline

- Introduction to Project
- Problem Formulation
- Objectives of the work
- Methodology used
- Results and Outputs
- Conclusion
- Future Scope
- References

Introduction to Project

The rapid advancement of surveillance technologies has led to concerns about privacy infringement and data misuse. Traditional surveillance systems often collect and store large amounts of personal data, raising privacy issues and ethical concerns.

The project "**Privacy-Preserving Surveillance System**" aims to create a surveillance system that can monitor and protect areas while minimizing privacy concerns. Traditional surveillance systems often collect and store large amounts of personal data, raising privacy issues and ethical concerns.

Identify the key privacy concerns related to surveillance, such as facial recognition, tracking, or data storage. Ensure your system complies with relevant privacy regulations (e.g., GDPR, CCPA).

Introduction to Project

The project focuses on the following parameters:

- Use privacy-preserving technologies in video analytics surveillance systems which is crucial for protecting individuals' privacy.
- Determine the technologies and protocols to be used for each component, considering factors such as security, scalability, and interoperability.
- Identify and implement advanced encryption techniques, such as homomorphic encryption.
- Develop mechanisms for access control, authentication, and auditing to ensure that only authorized users can access the surveillance data.

Problem Formulation

- Design and develop a surveillance system that effectively monitors and protects areas while minimizing privacy concerns related to data collection, storage, and analysis.
- Demonstration of effective data anonymization techniques that protect the identity of individuals captured in surveillance footage.
- Implementation of robust data security measures, including encryption during transmission and storage.
- Development of a user-friendly interface that allows for easy monitoring and management of the surveillance system.
- Successful deployment of the system in a real-world setting, with positive feedback from users and stakeholders regarding privacy protection and system performance.

Objectives of the Work

The Aim and objective of the project is :

- To design and implement a privacy-preserving surveillance system that can monitor and secure public or private spaces without compromising individual privacy rights.
- To create a system that prioritizes privacy by incorporating techniques such as data anonymization, encryption, and minimization of data collection, while ensuring compliance with relevant privacy regulations and ethical standards.
- Implement machine learning algorithms for object detection, tracking, and anomaly detection while preserving privacy through techniques like federated learning or differential privacy.

Scope of the Project

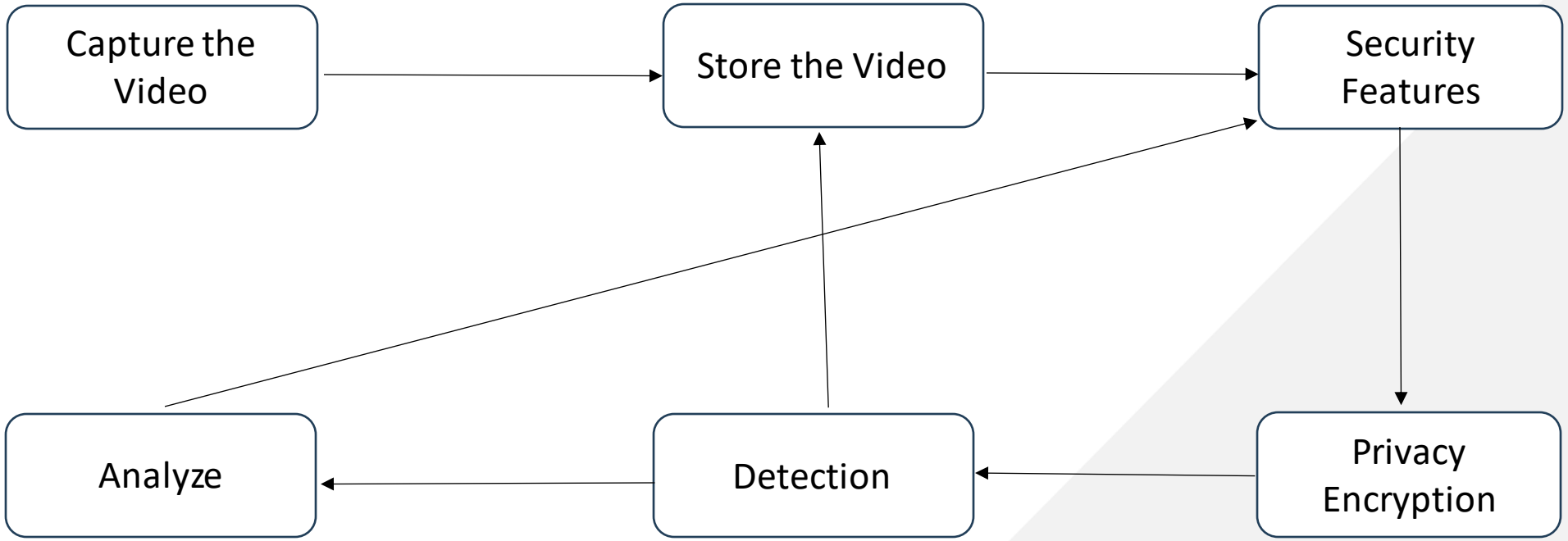
- Conducting thorough testing to ensure the system meets privacy requirements and performs effectively in real-world scenarios. This includes testing for data anonymization effectiveness, encryption strength, and system performance under different conditions.
- Implementing different security measures to protect surveillance data against unauthorized access, manipulation, and data breaches by using various means such as Access Controls, Auditing Mechanisms, etc.
- Design user-friendly interfaces for accessing, monitoring, and analyzing surveillance data. Provide visualization tools and dashboards for presenting insights and analytics.

Methodology used

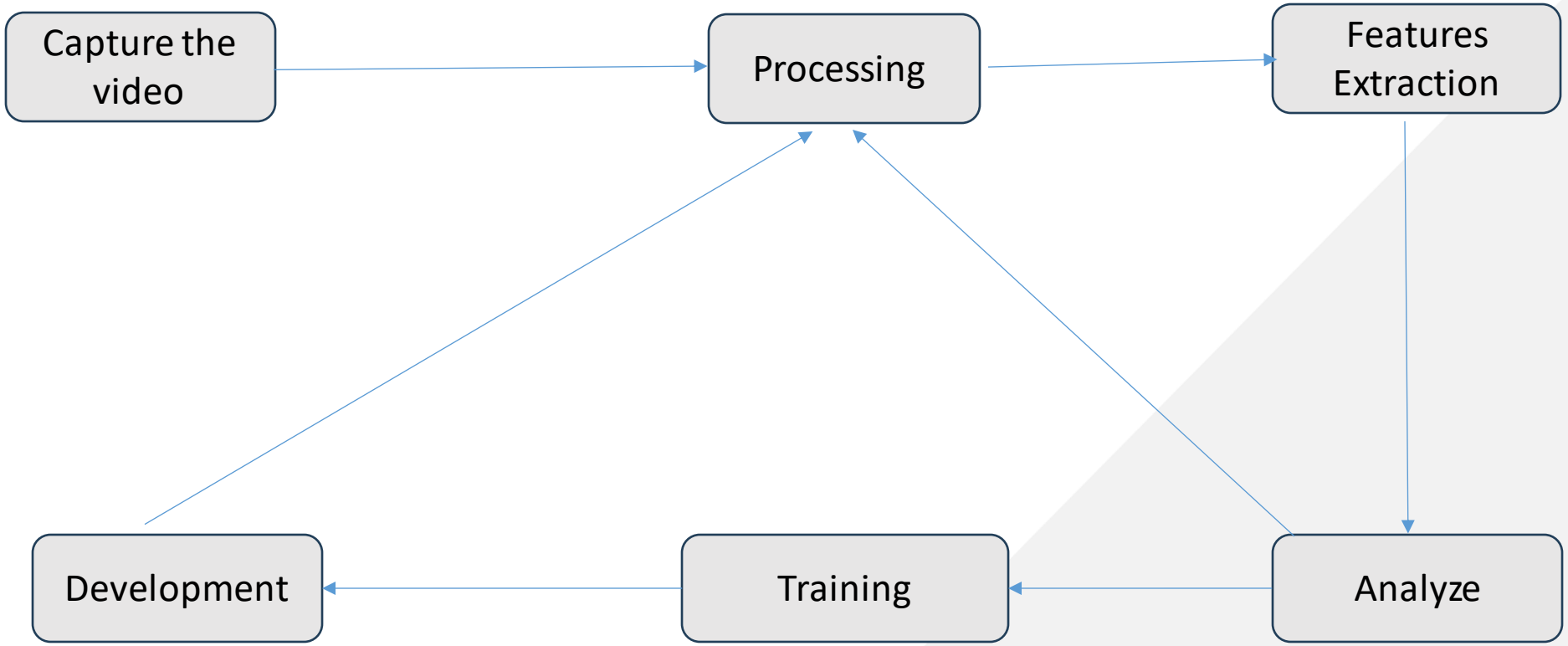
The methodology for the "**Privacy-Preserving Surveillance System**" project involves a systematic approach to designing, developing, and implementing the surveillance system while prioritizing privacy considerations. Here's a general outline of the methodology:

Firstly we will capture the video, and then store it in our storage source, implementing security features such as encryption to provide security to the video, and analyze the data for future use.

Methodology Used



Design


Capture the video
Processing
Features Extraction
Development
Training
Analyze

Results and Outputs

```
Enter username: User1
Enter password: Admin@123
Authentication successful.
Displaying menu...
```

Fig.1: Authentication

```
Menu:
1. Live video surveillance with face detection
2. Face matching from image with live video surveillance
3. Face matching from image with stored video
4. Homomorphic encryption and decryption
5. Pseudonymous technique
6. Exit
```

Fig.2: Main Menu

```
Enter your choice: 1
Selected choice: 1
Executing live_face_detection...
```

Fig.3: Choice Selection

```
Enter your choice: 2
Selected choice: 2
Executing face_matching_live...
Enter the path to the reference image: C:\Users\micro\Pictures\Camera Roll\pic.jpg
Do you want to store the most accurate matched face? (yes/no) : yes
Enter the storage location with a valid file extension (e.g., D:/matched_face.jpg): D:\Output\Output_option2.jpg
```

Fig.4: Processing

Results and Outputs

```
Menu:
1. Live video surveillance with face detection
2. Face matching from image with live video surveillance
3. Face matching from image with stored video
4. Homomorphic encryption and decryption
5. Pseudonymous technique
6. Create a new user account
7. Exit
Enter your choice: 2
Selected choice: 2
Executing face_matching_live...
Enter the path to the reference image: C:\Users\micro\Picture
s\Camera Roll\pic.jpg
Do you want to store the most accurate matched face? (yes/no)
: yes
Enter the storage location with a valid file extension (e.g.,
D:/matched_face.jpg): D:\Output\Output_option2.jpg
Most accurate matched face stored successfully.
Face matched with 91.67% accuracy.
```

Fig.5: Result

```
Menu:
1. Live video surveillance with face detection
2. Face matching from image with live video surveillance
3. Face matching from image with stored video
4. Homomorphic encryption and decryption
5. Pseudonymous technique
6. Create a new user account
7. Exit
Enter your choice: 6
Selected choice: 6
Creating a new user account...
Enter new username: user
Enter new password: user
Enter role (admin/viewer/writer): viewer
Enter permissions (comma-separated): live_face_detection
User account created successfully.
```

Fig.6: User Creation

Results and Outputs

	username	password	role	permissions
	Filter	Filter	Filter	Filter
1	User1	Admin@123	admin	create_user,live_face_detection,face...
2	User3	Viewer@123	Viewer	live_face_detection
3	User2	Writer@123	writer	homomorphic_encryption_decryption,...
4	user	user	viewer	live_face_detection

Fig.7 Credentials database

timestamp	event	user_info
Filter	Filter	Filter
2024-04-20 22:43:56	Live video surveillance with face ...	admin

Fig.8 Log File for managing Events

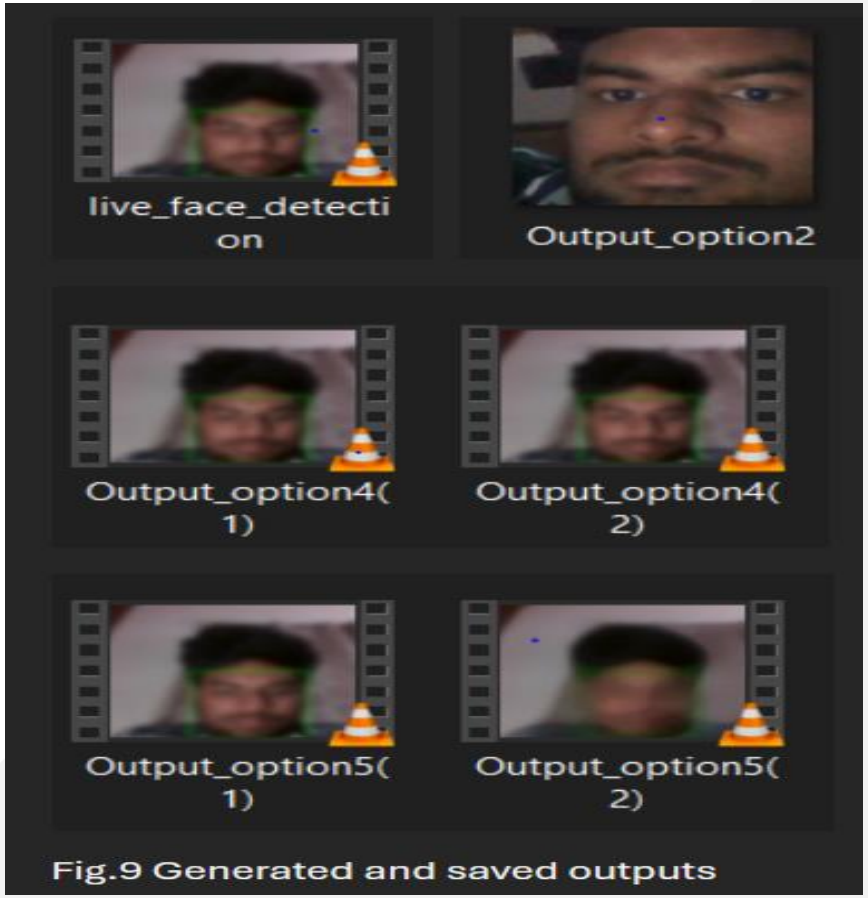


Fig.9 Generated and saved outputs

Conclusion

In conclusion, the privacy-preserving surveillance system presented in the code represents a sophisticated solution to the security and privacy challenges inherent in surveillance applications. By integrating access controls, encryption techniques, and pseudonymization methods, it provides a comprehensive approach to safeguarding sensitive data and preserving individual privacy rights. With ongoing refinement, adherence to regulations, and user acceptance, the system holds promise as an effective tool for ensuring public safety while upholding privacy standards in our increasingly digital age.

Future Scope

The future scope of the privacy-preserving surveillance system outlined in the provided code is promising and multifaceted. Here are several potential avenues for its development and application:

- Continuous advancements in encryption and pseudonymization techniques can further bolster the system's privacy capabilities.
- Integration of machine learning algorithms for anomaly detection and behavior analysis can augment the system's surveillance capabilities.
- Promoting user education and awareness about the system's privacy-preserving features will be essential for fostering acceptance and trust.
- Collaboration with academia, industry partners, and regulatory bodies can drive ongoing research and development efforts.

References

- Zheng, S., Ren, Y., Xiong, H., & Wang, Y.: "Privacy-preserving face recognition in surveillance videos using deep learning and homomorphic encryption". Multimedia Tools and Applications, 79(47-48), 35795-35816. (2020).
- Xu, Y., Wang, H., Wu, H., & Xiong, H.: "Privacy-preserving video surveillance using federated learning and differential privacy". IEEE Transactions on Multimedia, 23(11), 2469-2480. (2021).
- Wang, J., Zou, D., Wu, H., & Xiong, H.: "A privacy-preserving video surveillance system based on secure multiparty computation". Multimedia Tools and Applications, 78(4), 4627-4642. (2019).
- Zhang, Y., Xiong, H., & Wu, H.: "Privacy-preserving visual surveillance based on blockchain and federated learning". IEEE Transactions on Industrial Informatics, 17(4), 2968-2976. (2021).
- Chen, Y., Luo, J., Shen, L., & Xiong, H.: "Privacy-preserving facial expression recognition based on blockchain and federated learning". IEEE Transactions on Industrial Informatics, 17(10), 7260-7268. (2021).
- Kwak, H. Y., Lee, J., Moon, J., & Song, B.: "Privacy- preserving face recognition system using federated learning and differential privacy". Journal of Ambient Intelligence and Humanized Computing, 12, 1587-1597. (2021).
- Xiong, H., Wu, H., & Wang, J.: "Privacy-preserving visual surveillance using blockchain-based federated learning". IEEE Transactions on Circuits and Systems for Video Technology, 31(1), 338-349. (2021).
- Zhang, L., Chen, C., Zhang, S., & Xiong, H.: "A privacy- preserving surveillance system based on federated learning and homomorphic encryption". Journal of Visual Communication and Image Representation, 80, 102892. (2021).

References

- Zhang, Y., Jiang, Y., Xiong, H., & Wang, J.: "Privacy-preserving crowd counting based on federated learning and differential privacy". IEEE Transactions on Multimedia, 23(12), 3453-3465. (2021).
- Zhou, L., Wu, H., Wang, J., & Xiong, H.: "Privacy-preserving traffic sign recognition using federated learning and blockchain". IEEE Transactions on Vehicular Technology, 70(9), 9022-9032. (2021).
- Zhao, J., Chen, C., Chen, M., & Xiong, H.: "A privacy-preserving visual surveillance system based on blockchain andsecure multiparty computation". Journal of Real-Time ImageProcessing, 19(3), 1059-1074. (2022).
- Wang, J., Zhou, L., Wu, H., & Xiong, H.: "A privacy-preserving smart parking system based on federated learning and blockchain". Journal of Parallel and Distributed Computing, 160, 99-107. (2022).
- Yan, Q., Wu, H., Wang, J., & Xiong, H.: "Privacy-preserving human activity recognition using federated learning and blockchain". IEEE Transactions on Emerging Topics in Computing, 10(1), 214-224. (2022).
- Chen, C., Liu, K., Wu, H., & Xiong, H.: "Privacy-preserving visual object detection based on federated learning and blockchain". IEEE Transactions on Sustainable Computing, 7(1), 124-134. (2022).
- Li, W., Li, Y., Tang, Z., & Zhang, H.: "Privacy-preserving intelligent surveillance: A survey". Information Fusion, 75, 113-131. (2022).
- Chen, C., Zhou, L., Wu, H., & Xiong, H.: "Privacy-preserving pedestrian detection using federated learning and blockchain". Future Generation Computer Systems, 126, 399-409. (2022).

References

- Yang, Y., Li, W., Jiang, S., & Tang, Z.: "A survey of privacy- preserving techniques for visual surveillance systems". ACM Computing Surveys (CSUR), 55(1), 1-37. (2022).
- Zhang, L., Wang, J., Xiong, H., & Wu, H.: "Privacy- preserving facial recognition in surveillance videos using federated learning and differential privacy". Sensors, 22(2), 524. 2022).[31] Huang, L., Jiang, Y., & Wang, J.: "Privacy-preserving crowd behavior analysis using federated learning and differential privacy". IEEE Transactions on Cybernetics, 52(6), 2834-2846. (2022).
- Chen, C., Wu, H., & Xiong, H.: "A privacy-preserving visual surveillance system based on federated learning and secure aggregation". Journal of Parallel and Distributed Computing, 159, 65-74. (2022).
- Wu, H., Wang, J., Xiong, H., & Zhou, L.: "Privacy-preserving object tracking using federated learning and blockchain". IEEE Transactions on Multimedia, 24(2), 601-612. (2022).
- Zhou, L., Chen, C., & Wu, H.: "Privacy-preserving video summarization using federated learning and differential privacy". Multimedia Tools and Applications, 81(5), 7459-7473. (2022).